Published and Copyright (c) 1999 - 2015
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1734 09/11/15

~ US Cop Goes Wardriving ~ People Are Talking! ~ Sega Financials Poor!
~ System 6.0.3 Released! ~ Internet Freedom Dying ~ China Arrests 15,000!
~ Epson Kills Ink Cart! ~ 'Fallout 4' Will Grow! ~ Mt. Gox'er Arrested!

~ PlayStation Saves Sony ~ No Consent for Win 10? ~ iTunes Illegal in UK!

-* Graphical OS for Atari 8-bit *-
-* Atari Coldfire: The New Series 2015 *-
-* Russian Hacker Group Exploits Satellites! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

As you’ve all probably already been reminded countless times today already, today marks the 14th anniversary of the World Trade Center tragedy, as well as the carnage at the Pentagon and in Shanksville, Pennsylvania. The world - especially the United States - as we knew it, changed forever. I don’t think that any of us who "witnessed" that day’s events will ever forget those tragic scenes. If you haven’t already, take a moment to reflect on that fateful day and remember all of those who lost their lives needlessly.

Until next time...

=~=~=~=

Atari Coldfire: New Series 2015

Dear All,

Yesterday the 25th preorder arrived our team. So half of the needed preorders for the new series of FireBee boards are in now! That’s especially great as it is just 2 weeks since we published the call for preorders. And 80% of the people wanted to make a prepayment as well. You are great!

So please go on for the next 25 preorders that are needed before we can go into production. I would like to ask you as well to update your links to the new website firebee.org at your own websites, blogs or whatever and perhaps to spread the information about the new series.

At least it is a kind of community project where nobody earns anything ;)

Mathias

Atari-coldfire mailing list
Atari-coldfire@lists.lnxnt.org

https://lists.lnxnt.org/mailman/listinfo/atari-coldfire

A Graphical OS for the Atari 8-bit

Atari 8-bit fans have long hankered after a GUI similar to GEOS on the Commodore 64. Diamond GOS went some way to addressing this deficiency, and since then there have been several creditable attempts at implementing a GUI OS on the A8. Now there s another one in the pipeline: an as yet unnamed project which aims to bring a pre-emptive multi-tasking graphical operating system to the 8-bit Atari.

The most recent demo version of the GUI OS can be downloaded below:

http://atari8.co.uk/wp-content/uploads/2015/03/GOS-ROMs.zip

The ZIP file contains ROMs and ATR flashers for a variety of popular programmable cartridges, and separate versions are provided for use with Atari ST and Commodore Amiga mice.
Info

The GUI/OS project grew out of a simple mouse demo, based on the interrupt driven mouse handler by John Maris. However, thanks to ideas and help from AtariAge members analmux, andym00, and popmilo, a simulated hi-res hardware sprite pointer was developed, of which the underlying application is completely unaware.

Meanwhile, Paul Fisher took on full responsibility for font design and production (creating a tool-chain for converting BDF fonts for use with our GUI), and has designed several hundred icons and dozens of other resources. He is also chief beta-tester, and without Paul s assistance, this project would have been an impossible undertaking. Paul has also created several developmental screen mock-ups which depict how the finished product is likely to look. The mock-ups are realistic representations of screen elements currently being implemented. The completed graphical OS will include:

- A pre-emptively multitasking kernel supporting up to 16 processes
- Inter-process messaging system, supporting up to 64 open messages
- Completely replaces the Atari OS and DOS
- File system drivers supporting FAT12, FAT16 and FAT32
- Overlapping, movable, sizeable windows
- Cascading pull-down and pop-up menus
- Movable desktop icons and shortcuts
- Per-process and overall CPU load profiling
- Dialogue boxes with a rich control set (list boxes, spinners, sliders)
- 256 character fonts from 6 to 32 points
- Italic, boldface, and underline, outline, and shadow styles for all fonts
- Smooth, quick and responsive mouse control
- Desktop file manager with drag-and-drop support

Comprehensive API and technical documentation for developers

While it is hoped that the OS will support unexpanded 64KB XL/XE machines in some minimal way, the realistic base hardware requirement will be an 8-bit Atari XL/XE with at least 128KB, a flash cartridge (or Ultimate 1MB/Incognito), and an ST or Amiga compatible mouse or trackball.

In late 2012, Jörn Mika (aka Prodatron), author of the remarkable SymbOS Graphical Operating System for the CP/M, MSX and other Z80 platforms, approached me with some suggestions regarding rendering, window management and multi-tasking. Because of those pivotal conversations and the insight Jörn provided, the decision was made to abandon the A8 GUI s right-threaded binary tree internal object structures (initially modelled after TOS on the ST), and adopt instead flat window records almost identical to those used by the SymbOS API. This change immediately yielded considerable reductions in code complexity and size, and an increase in efficiency. But yet there was still room for improvement in other areas.

After a further six months of nagging doubts about the proprietary window mask technology I had designed, I decided to take the plunge and do what Jörn had suggested might lead to a considerable increase in rendering speed: namely, to abandon the window masks (which, it turned out, might as well have been called regions), and use a traditional dirty-rectangle window management system, as used in SymbOS. In summer/autumn 2013 I set about writing a full implementation of the rectangle-based window manager. Impressed with the result, I committed to the change and optimised the whole system to use the rectangles, and this massive rewrite resulted in a roughly 100 per cent efficiency improvement when rendering the content of overlapping windows. After further optimisation of the font renderer, we finally began to see performance which appeared to approach that of the seemingly magical SymbOS.

In addition to this, Jörn convinced me that pre-emptive multitasking was possible on the 6502, so in May 2014, I began the arduous task of converting the existing code to run from a bank-switched cartridge, while simultaneously designing the pre-emptively multitasking kernel. As of August 2014, the cartridge build is working well and the kernel is fully functional, and we can finally witness multiple tasks sharing CPU time on the 8-bit Atari, and using a messaging queue for communication. Thanks to Jörn and many members of the AtariAge forum, some really inventive techniques of stack and page zero management have been implemented.

What is especially heartening at this stage is that the 8-bit Atari can actually run a pre-emptive scheduler, and run it well in spite of the 6502 s fixed stack. And the Atari s custom hardware has made some other really nice things possible, such as the calculation of processor usage on a process-by-process basis, as well as the monitoring of CPU idle time.

To help potential developers, documentation of the API will continue throughout 2015/2016, and perhaps unsurprisingly this task becomes easier as the architecture of the system

becomes more clearly defined while it s being coded up. There s still a lot of work to do (UI controls, file system, SIO driver, etc), but now that we have a rudimentary multi-tasking graphical OS and one which is efficient and usable there seems to be no limit to what is achievable.

Donations

If you want to show your support for this project and help to ensure it s seen through to completion, please consider making a donation. Progress has been slow because my free time is in contention owing to the other Atari projects documented on these pages, but I hope to maintain a clear focus on the GOS project in the future.

The Source Awakens .. System 6.0.3, A New Release

On the heels of the recent 6.0.2 build of the Apple IIgs System Disk set, comes the next revision. Many loose ends have been tied up and documentation has been updated with changes described in detail.

This release has been packaged as six 800K disk images in BXY format (Shrinkit Compatible Binary II Encoded), .PO format, and as a versatile 32MB Live Installer in .PO format that boots to Finder for immediate access to all portions of the System Software and installing without the need of mounting multiple images or swapping floppies. This image can also be installed to a 32MB partition, CD ROM, etc.

Apple II Technical Notes Apple IIgs #001 and GS/OS #100 have been updated to reflect the content and organizational changes in this release.

See the file: Apple_IIGS_6.0.3_Info.txt for the individual image names/contents.

This is a summary of the visible changes since System 6.0.2 was released. Be sure to also read the Shortcuts file on the Live.Install or SystemTools2 disk for more information.

SCC.Manager and the AppleShare FST no longer halt the boot process with dialogs requiring user intervention when the machine is not connected to a network. These warnings are still available by pressing the spacebar during boot to view the text boot screen.

OpenApple-Up Arrow now selects the folder or volume icon of the directory from which it was invoked.

A Live Install image is now available, enabling installation of the System Software from a single disk image rather than the traditional six 800K floppy disks.

In the Live Install image only, a Customized Installer application is now available for the use of developers.

Selection, deletion, and traversal of Japanese full-width (double byte) characters and words is handled correctly when the Japanese Manager is installed and active.
Word breaks recognized by Option-Left/Right Arrow, and double-clicking now include punctuation and symbols, rather than just spaces. Hyphen (-), period (.) and apostrophes (and closing single smart quote) are considered word breaks when not surrounded by alphanumeric characters, but are not considered word breaks when they are. For example, the following constitute a single word:
flip-flop?don t?foo.txt

All other non-alphanumeric characters are excluded from words. Double-clicking on a word break causes it and any surrounding word break characters to be selected. Traversing a word break using Option-Left/Right Arrow will pass through any preceding or following word breaks, stopping at the boundary of the next word encountered.

TextEdit (document window) and LineEdit (dialog box text fields, Finder icon rename fields) now use the OpenApple and Option keys in the same way. Previously, TextEdit used OpenApple for word navigation and Option for line and page end navigation.

Time control panel?Now follows the US Daylight Savings Time based on the standard effective March 2006.

FindFile?When used in the Finder, double-clicking any found file will open a window with the file selected.

Teach 1.1.1 is included, fixing a bug that caused an I-beam instead of an arrow cursor to display when mousing over the left border of the scrollbar.

The Thunderclock year table in P8 has been updated for the years 2013-2018. There is also a Clock.Patch file on the SystemTools2 disk that you may use to update P8 (renamed to ProDOS) to include future year groups.

Apple IIGS Technical Note #100 and GS/OS Technical Note #001 have been updated for System Software 6.0.3.

=~=~=~=

->In This Week’s Gaming Section - How ’Fallout 4’ Will Grow and Evolve!
  """""""""""""""""""""""""""""""   Here’s Why The PlayStation Will Save Sony!
                                    SEGA Financials Report Dramatic Decrease in S
ales!

=~=~=~=

Here's How 'Fallout 4' Will Grow and Evolve After It Launches

When Fallout 4 arrives on Nov. 10, that's just the beginning. Developer Bethesda Softworks has big plans for the game post-release, which are starting to trickle out.

Here's the big ticket reveal: Bethesda plans to release studio-created add-on content for Fallout 4 in the months after its release, and it'll be offered in a packaged $30 "Season Pass" deal. There's no mention of a plan to sell the add-ons individually, but that's likely an option as well. You'll just be paying more if you buy everything piecemeal.

"Since we re still hard at work on the game, we don t know what the actual [downloadable content] will be yet, but it will start coming early next year," a new post on Bethesda.net reads. "Based on what we did for Oblivion, Fallout 3, and Skyrim, we know that it will be worth at least $40, and if we do more, you'll get it all with the Season Pass."

The same post also elaborates a bit on Fallout 4's planned support for user-created "game mod" modifications. It's a common practice in the PC gaming world for amateur programmers to tweak and add different elements to their favorite games, but Fallout 4 will be one of the first to bring support for those unofficial add-ons to PlayStation 4 and Xbox One consoles.

Early next year we ll release for free the new Creation Kit for the PC," the post continues. "This is the same tool we use in the studio. You'll be able to create your own mods and share them with others. We re especially excited these same mods will then be coming to Xbox One, and then PlayStation 4."

All of this echoes what Fallout 4 game director Todd Howard told Mashable at E3 back in June: an early 2016 release for the PC Creation Kit, then on to Xbox One first "The best path for us is to do it there first," Howard explained and, finally, PS4.

"How those all line up, what's the gap between PC and Xbox, and Xbox and PS4, is a little fuzzy right now. But that's definitely the order," Howard told Mashable.

Finally, in what should be no surprise to fans, Bethesda carries forward the "free content updates" mentality that was born with its previous game, The Elder Scrolls V: Skyrim. In addition to a regular flow of patches that fix bugs and other issues, fans can also look forward to free in-game bonuses in addition to the planned add-ons.

"For Skyrim, we added things like mounted combat, legendary mode, kill cams, visual enhancements and more," the Bethesda.net post said. "We ll work with all of you to figure out what new things you d love to see added to Fallout 4, whether they are small tweaks or new features."

20 Years Later, Here’s Why The PlayStation Will Save Sony

Sony s game console went on sale in the U.S. on Sept. 9, 1995. Today it s a linchpin for the company s future.

Twenty years ago, the Sept. 9, 1995 U.S. release of Sony s PlayStation ushered in momentous changes to the video game industry and set the company on a path to becoming a superpower in the entertainment field.

The system had made its global debut in Japan in December 1994 and was an instant hit there, selling 2 million units in the first six months. But by launching sales in the larger U.S. market, the PlayStation became a global phenomenon, ultimately knocking Nintendo off of its perch as the industry leader and ushering in a new distribution method for video games that continues to evolve today.

Sony brought a super friendly and encouraging approach to developers and third party publishers in a way that Nintendo did not, says John Taylor, managing director of Arcadia Investment Corp. Back in the old days, when Nintendo and Sega dominated the market, there were these things called slots. Publishers were restricted to releasing a set number of titles. Sony brought open arms and a lot of flexibility to the model.

That openness won the PlayStation a lot of support from third-party publishers, like Electronic Arts EA -1.05% . But the success of the console ultimately can be traced to two important firsts. It ushered in the era of 3D graphics and it was the first game machine to focus on the CD as a storage medium, rather than clunky cartridges.

Using CDs greatly reduced manufacturing costs with publishers paying between $1.50 and $2 per disc at the time instead of $8-$12 for chip-based cartridges. It also gave retailers more flexibility on close-out pricing, letting them offer deeper discounts on older games.

Ironically, Sony SNE 0.64% never really wanted to go into the video game business at least not the way it ultimately did. In 1988, Sony had hoped to partner with market leader Nintendo NTDOY -0.40% on a CD-ROM player for the SNES. Three years later, Sony debuted the machine at CES.

But the day after that reveal, Nintendo dropped a bombshell, declaring it would not work with Sony and would instead partner with Phillips. Furious at the slight, Sony then-president Norio Ohga assigned Ken Kutaragi to develop a system that would compete with Nintendo.

As tempers cooled internally, Sony began to second guess the directive as officials grew skeptical about the profitability of the video game industry, but Kutaragi successfully lobbied to keep the project alive.

The mid- 90s were an exciting time for game developers, driven by the explosion of powerful but affordable 3D graphics rendering hardware and the birth of many young and adventurous development studios, said Shuhei Yoshida, president of Sony Computer Entertainment Worldwide Studios in a blog post last year. The original PlayStation was meant to embody that sense of adventure and discovery, that sense that anything was possible.

Today, the PlayStation is a lynchpin in Sony s future plans. The most recent iteration of the system the PS4 has sold more than 25 million units life to date.

Sony CEO Kaz Hirai (who ran the PlayStation division during the glory days of the PlayStation 2) has made it clear that he sees the console as one of the tentpole divisions that will lead the company back to prosperity. Since the early 2000s, the company has been losing ground in many fields. Rivals like Samsung took away market share from the company s electronics business. Apple and others dominated the portable music space. And the company s ADR stock fell below $10 in 2012.

Hirai s turnaround efforts are starting to bear fruit. One of the keys to that is his use of the PlayStation 4 as a way to break down the company s silo mentality integrating marketing efforts for other units, like film and music, into it to create a more cohesive entity.

Sony made hay on the Walkman decades ago, says Taylor. And it made hay on TV sets a decade or two ago. But the one dependable, bankable division providing both industry leadership and profitability has been the PlayStation division.

SEGA Financials Report Dramatic Decrease in Sales

Reporting a decrease of 42 percent in net sales, the publisher reports sales earnings of ¥52.9 billion ($426 million), operating losses of ¥9.5 billion ($76 million), and net losses of ¥7.9 billion ($63.8 million).

SEGA representatives largely attribute the decrease in sales figures to global economies, with additional issues arising from the reported decrease in demand for game software, amusement centers, and amusement machines in Japan.

"The economy still remained in the condition requiring further time for full recovery due to uncertainty towards a downswing in overseas economies arising from factors such as the slowdown of growth in the economies of emerging countries and European debt crisis," SEGA said.

The company announced plans of downsizing and relocating its offices in North America earlier this year, issuing redundancies in their Japanese, European, and North American offices.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

China Police Arrest 15,000 Suspects for Alleged Cyber Crimes

China Police has arrested nearly 15,000 people on suspicion of cyber crimes as part of an operation dubbed "Cleaning the Internet," according to reports.

According to the Chinese Ministry of Public Security (MPS), the suspects have been arrested for their involvement in cyber crimes that "jeopardized Internet security."

In July, China launched a six-month campaign codenamed "Cleaning the Internet" to fight online criminal activities.

Under the program, the police investigated 7,400 cases, including hacking, online fraud and the illegal sale of personal information, spread over 66,000 websites, the official website of the ministry stated.

"For the next step, the public security organs will continue to increase their investigation and crackdown on cyber crimes," according to the Chinese Ministry of Public Security.

The MPS did not clear exactly when the arrests took place but said the program also took down major online criminal cases as well as eliminated online gangs.

Police suspended more than 190,000 illegal online websites featuring vulgar contents including advertisements for pornography, firearms, explosives, and gambling.

China is considered to be a country that took the Internet as their virtual territory; a territory that must be ruled by government’s laws and regulations. It’s also the country that runs one of the world s most sophisticated Internet censorship systems called The Great Firewall.

Russian Hacker Group Exploits Satellites To Steal Data, Hide Tracks

A Russian-speaking hacking group is using commercial satellites to steal sensitive data from military and diplomatic agencies in the United States and Europe, according to Kaspersky Lab.

Washington: A group of sophisticated Russian-speaking hackers is exploiting commercial satellites to siphon sensitive data from diplomatic and military agencies in the United States and in Europe as well as to mask their location, a security firm said in a new report.

The group, which some researchers refer to as Turla, after the name of the malicious software it uses, also has targeted government organisations, embassies and companies in Russia, China and dozens of other countries, as well as research groups and pharmaceutical firms, said Stefan Tanase, senior security researcher at Kaspersky Lab, a Moscow-based cybersecurity firm with analysts around the world.

Turla has used this technique for at least eight years, which reflects a degree of sophistication and creativity generally not seen among advanced hacker groups, Tanase said.

"For us, it was very surprising," he said in a phone interview from Bucharest, Romania. "We've never seen a malicious operation that hijacked satellite" connections to obtain data and to cover its tracks. "This is the first group that we believe has done it. It allows you to achieve a much greater level of anonymity."

Although Kaspersky has not linked Turla to the Russian government, other security firms have done so.

The Turla malware originated from a "sophisticated Russian-government-affiliated" hacker group that "we call Venomous Bear," said Dmitri Alperovitch, co-founder and chief technology officer of CrowdStrike, an Irvine, California-based cybersecurity technology firm.

Turla specialises in diplomatic and military targets in the United States, Europe, Middle East and Central Asia to gain political and strategic intelligence, he said. Turla is not the Russian group that is believed to have hacked the State Department, White House and Pentagon over the past year, Alperovitch said. That group was dubbed Cozy Bear by CrowdStrike.

Turla's tactic exploits the fact that older satellites do not encrypt data streaming to Earth, and it relies on unsuspecting users of satellite internet service providers around the world, Tanase said.

Here's how the scheme works: Turla infects a target's computer by planting malicious software on a website that the group knows the user frequents. When the user visits the site, his computer is compromised. This is called a "watering hole" attack.

Once Turla has gained control of the user's computer and identified data of interest, the hacker instructs the infected computer to send the stolen data to the internet address of an innocent satellite user - someone who is online using internet service provided by the satellite company.

Turla then hijacks the stream of data as it is being sent down from the satellite to the innocent user's computer by spoofing the user's internet address. The data is sent to a command server controlled by Turla, but the location is effectively hidden as it can be anywhere in the range of the satellite beam, which can be thousands of kilometres.

Moreover, Tanase said, Turla tends to use satellite internet connections in Middle Eastern and African countries. He thinks

this is an effort to avoid the scrutiny of researchers and law enforcement.

To use such connections, Tanase said, the hackers need to have at least an antenna and a computer there. "They must have people posted in these countries" for technical support, he said. He noted that the group has exploited satellite internet providers located in Afghanistan, Congo and Libya, among others.

Tanase said Kaspersky has asked the satellite service providers whether they could block the malicious traffic, but they said their hands were tied. "This is a limitation of the technology," he said.

The problem will be solved over time as these satellites are replaced with new ones, he said. "But until then," he said, Turla's data hijacking "will still be possible."

US Cop Goes Wardriving To Sniff Out Stolen Gadgets by MAC Address

When it comes to sniffing out unsecure Wi-Fi networks, you can take your pick of vehicle to drive around: we've had warbiking, feline warprowling (with bonus mouse catching!), and warstrolling (with high heels packing Wi-Fi hacking tools, no less!).

Now, a US cop has reverted to the plain old vanilla mode of wardriving in a car, but he's not looking for hotspots or routers that lack passwords.

Nor is he sniffing out routers using the creaky, old, easily cracked WEP encryption protocol.

Rather, Iowa City police officer David Schwindt is stalking stolen gadgets.

Specifically, he's cooked up some software and rigged up a thumb drive sized-antenna that plugs into the USB port of his squad car laptop to sniff out the media access control (MAC) addresses from a database of known stolen items.

MAC addresses are unique identification numbers that act like a device's digital fingerprint.

Researchers have confirmed they also link to your real identity, and, according to Edward Snowden, the National Security Agency (NSA) has a system that tracks the movements of everyone in a city by monitoring the MAC addresses of their electronic devices.

Schwindt says his software product, which he's calling L8NT - that's a leet-speak/acronym hybrid that stands for latent analysis of 802.11 network traffic - won t be used to find the occasional stolen iPod or laptop.

Neither will the tool give police access to personal or private information included in MAC packets, he told The Gazette.

Rather, he has his eye on bigger cases:

> If your cellphone is stolen from a bar ... that s not necessarily what L8NT is intended for. But, if your home is burglarized and your cellphone is stolen, now, as a police chief, I m interested [in that technology.]

The device - which has a range of about 300 feet - scans for MAC addresses, looking for matches to known stolen items.

The L8NT can also be attached to a directional antenna to allow police to determine where the signal is coming from and to obtain a warrant.

However, the device does not work in all circumstances.

If you walk around with Wi-Fi enabled on your phone, it will broadcast its MAC address indiscriminately and, unlike an IP address which changes over time or when you switch networks, a MAC address is constant (though it can be spoofed, either for legitimate purposes or by a thief who wants to hide it).

But if a device is powered down, or if Wi-Fi has been disabled, the L8NT won't be able to sniff it out.

Nor will it do much good if legitimate device owners haven't bothered to record the MAC addresses of their devices.

Then again, it might also prove useless in the case of Apple's iOS 8 devices.

Apple introduced a random MAC address generator in iOS 8 last year, in an effort to help users fend off marketers' ability to recognize their devices and thereby ID them at will.

That randomisation isn't constant, mind you: As Paul Ducklin noted at the time, randomisation only happens before you connect, when your Wi-Fi card is scanning for networks.

When your iGadget finds an access point with a name that matches one of your known networks, it tries to connect by using your real, rather than your random, MAC address.

So the coffee shop you visit regularly won't have any trouble recognising you, though a shopping mall you merely walk through won't be able to ID you.

But while there are cases where the officer's L8NT won't work, Schwindt still has big plans, he's developed a proof of concept, has a provisional patent on the device, and plans to apply for a full patent this fall.

In the meantime, he's sent out surveys to law enforcement agencies to test the waters and see if they might be interested.

Mt. Gox Founder Mark Karpeles Arrested - But Not Over Missing Bitcoinage

From a marketing point of view, 2014 could have been a much better year for the cryptocurrency known as Bitcoin.

Bitcoin isn’t really a currency, at least in the traditional sense, because there’s no central regulatory authority that issues coins and banknotes or controls the total amount of the currency in circulation at any time.

In the Bitcoin world, "coins" are "minted" (or, more accurately, mined) by getting lucky in what is effectively an arithmetic lottery based on cryptography.

In place of an issuing authority with a list of all the banknote serial numbers that exist, Bitcoin revolves around a public, distributed database called the block chain that keeps a record of which "coins" have been mined so far, and how they’ve been spent.

The arithmetic in the Bitcoin system limits the total number of bitcoins that can ever be mined to about 21,000,000. The block chain acts as a pseudo-anonymous register of all bitcoins mined so far. This prevents two people coming forward and claiming to "own" the same coin, or part thereof. The block chain therefore acts as the Bitcoin ecosystem’s arbiter to stop people saying, "Hey, I never got paid," or, "Hey, I never spent that amount, it still belongs to me."

Ironically, that means Bitcoins are much safer under your metaphorical mattress than stored in an online account.

But unless you can find other people who are willing to trade bitcoinage with you directly, a Bitcoin stash isn’t very liquid - with some notable exceptions, you can’t simply jump online and spend it, or go into a shop and make an impulse purchase.

This has led to a proliferation of Bitcoin exchanges, where you can trade bitcoinage for regular currency, albeit at rather volatile rates.

Of course, that means that an exchange actually has to have real currency available for the times that customers want to convert some of their bitcoins into regular money.

It also means, if you want quick and easy access to your bitcoin account, that the exchange needs to keep at least some of your stash of digital money in what is known as hot storage essentially, accessible online where a determined hacker might very well be able to get at it.

With little or no regulation, and no central authority to repudiate disputed transactions or ownership, you aren’t going to get your hot wallet back if a crook makes off with it.

Responsible exchanges keep some, most, or even all, of your bitcoins (usually, you can choose how to divvy up your stash) in cold storage.

Cold wallets are supposed to to be offline, for example saved to removable storage devices and locked in a vault, just as the majority of the cash on hand might be be at a regular bank.

That doesn’t protect you against bitcoin crime entirely: an insider could steal your bitcoins, or an exchange’s idea of "offline storage" might not be quite as far removed from remote network access as you might like.

And, with little or no regulation, we’ve seen a procession of Bitcoin exchanges that have lost some or all of the digital assests in their possession, such as:
May 2012. An exchange called Bitcoinica allegedly had $225,000 stolen, followed by another $90,000 later the same year.

September 2012. $250,000 was stolen from boutique exchange Bitfloor after an encryption lapse during a server upgrade.

November 2013. Small exchanges in Australia, China and Denmark "vanished along with the money" after claiming they’d heen hacked.

March 2014. Poloniex lost $50,000 due to a coding error (known as a race condition) in its Bitcoin withdrawal database.

March 2014. Flexcoin closed down after hackers processed a fraudulent transfer of $600,000, with reports suggesting that was everything that Flexcoin had on deposit, gone in one shot.

But the Big Daddy of Bitcoin implosions was that of Mt. Gox, pronounced "Mount Gox," although originally a domain name that was short for MTG Gathering Online Exchange, a website devoted to the fantasy trading card game Magic: The Gathering.

And, just like magic in reverse, early in 2014, Mt. Gox, based in Japan, filed for bankruptcy.

The reason was the rather significant problem that the company had managed to "lose" about $500,000,000’s worth (half a billion dollars!) of its customers’ bitcoins.

What happened is still not clear, although a person claiming to be "Mt. Gox’s first employee" has recently commented at some length on Reddit what he claims is a partial explanation of how the company came to run out of money.

(NB. The Reddit thread makes fascinating reading, but there is no way to verify any of it, so: reader beware.)

Of course, running out of money by spending too much is not the same as losing 650,000 bitcoins.

The vanishing bitcoins still haven’t been explained, although a Japanese newspaper openly suggested, on New Year’s Day 2015, that 99% of the loss was an insider job: cybercrime committed by a person or persons inside the company.

Mt. Gox founder Mark Karpeles has always denied any wrongdoing, but he’s just been arrested anyway.

Apparently, Karpeles is not being charged over the missing bitcoins, but rather for overstating his financial position by US$1,000,000 back in February 2013.

The 650,000 missing bitcoins remain just that: missing.

Black Hat Keynote Speaker Says Dream of Internet Freedom Is Dying

The dream of a free and open Internet is slowly being killed by overregulation, censorship and bad laws that don’t stop the right people, a top computer crime defense lawyer says. The annual Black Hat computer security conference in Las Vegas kicked off Wednesday with a keynote address from Jennifer Granick, director of Civil Liberties at the Stanford Center for Internet and Society. Granick said that while the Internet needs to be reasonably safe in order to be functional, it’s no longer the revolutionary place it was 20 years ago.

No one is murdering the dream of an open Internet, she said, but it’s withering away because no one is prioritizing its protection. On top of that, new Internet users are coming from countries whose citizens aren’t protected by a Bill of Rights or a First Amendment. "Should we be worrying about another terrorist attack in New York, or about journalists and human rights advocates being able to do their jobs?" she asked.

Granick also railed against the federal Computer Fraud and Abuse Act, which carries sentences of up to 10 years in prison for a first-time offense. It does nothing to prosecute countries like China that launch state-sponsored attacks against the U.S. government and major companies, along with other dangerous hackers based overseas, she said. But, she added, it often hits small-time American hackers with unfairly harsh prison sentences.

In a separate briefing later Wednesday, Leonard Bailey, of the Department of Justice’s Computer Crime and Intellectual Property section, said that in most cases, prosecutions of computer crimes are very "reasonable" and not "prosecutors gone wild." "But all it takes is one flogging in the public square and there’s a chilling effect," he says. "So, we have to try to get this right."

A slew of hackers and information security professionals were slated to speak at Black Hat, including Charlie Miller and Chris Valasek, who gained fame recently by hacking into and taking control of a Jeep Cherokee, prompting Fiat Chrysler to recall 1.4 million vehicles to fix the problem.

iTunes Is Illegal Under UK Copyright Law

The High Court recently overturned private copying exceptions introduced last year by the UK Government, once again outlawing the habits of millions of citizens. The Intellectual Property Office today explains that ripping a CD in iTunes is no longer permitted, and neither is backing up your computer if it contains copyrighted content.

Late last year the UK Government legalized copying for private use, a practice which many citizens already believed to be legal.

The UK Intellectual Property Office noted that the changes were in the best interest of consumers and that they would bring copyright law into the 21st century.

However, the new regulation was short-lived. Fearing a loss of income several music groups objected at the High Court, which subsequently agreed that the new legislation is unlawful.

As a result the changes were overturned last month and the previous limitations were reinstated. To find out what the public can and can t do under the law, TF reached out to the UK Intellectual Property Office, which provided some very clear answers.

It is now unlawful to make private copies of copyright works you own, without permission from the copyright holder this includes format shifting from one medium to another, a spokesperson informed us.

The IPO specifically notes that copying a CD to an MP3 player is not permitted. This means that iTunes popular ripping feature, which Apple actively promotes during the software s installation, is illegal.

Also, under the current law iTunes is actively facilitating copyright infringement by promoting their CD-ripping functionality. This means that the company could face significant claims for damages.

There is more though, as the law affects much more than just ripping CDs. Simply copying a song in an automated computer backup or storing a copy on a private cloud hosting service is also against the law.

it includes creating back-ups without permission from the copyright holder as this necessarily involves an act of copying, we were informed by the Government spokesperson.

Strictly speaking this means that UK citizens are not allowed to make a backup of their computer. After all, pretty much every computer contains copyrighted media. Needless to say, this turns almost the entire country into outlaws .

The Government is not happy with the High Court decision but it hasn t decided whether it will propose revised private copying exceptions in the future.

Copyright holders previously suggested allowing private copying in exchange for a tax on blank CDs and hard drives.

As this is a complex area of law, the Government is carefully considering the implications of the ruling and the available options, before deciding any future course of action.

As reassurance, the Government notes that that people shouldn t be too concerned because copyright holders are not known to come after people who make a backup of their computers.

The Government is not aware of any cases of copyright holders having prosecuted individuals for format shifting music solely for their own personal use, the IPO spokesperson says.

However, copyright holders can take people to court over both CD-ripping and computer backups, if they want to.

Epson Kills the Printer Ink Cartridge

It was after midnight, and I was facing a ticking-clock real estate transaction. All I had to do was print 15 pages of black-and-white contract, sign it and fax it back. Only halfway through, my printer ran out of ink magenta ink! Thus began a chain reaction culminating in my nearly throwing the printer out the window. I ended up at Kinko s.

We all have a printer story. They run out of ink at the worst possible time, or worse, nag us about running low on ink when there s plenty left. So how much would you pay for a printer that doesn t run out?

Epson, the maker of my nightmare printer, has finally put an end to the horror of ink cartridges, at least for people willing to throw cash at the problem up front. The five new EcoTank series printers look like normal models, only they have containers on their sides that hold gobs and gobs of ink. How much? Years worth. Enough that your children or at least mine could go on a two-hour coloring-page-printing bender and you wouldn t even notice.

Printer technology has been pretty static for years. Epson and competitors Hewlett-Packard, Canon and Brother make frame-worthy photos and spit out page after page of text at a decent clip. It s now standard for them to connect to Wi-Fi networks and work with mobile devices.

Most people buy printers by price: $100 is the magic number for anybody but a photo enthusiast, and printer makers like it that way. They lose money on the hardware and make it up on ink.

We don t love paying through the nose for the ink, and the arrangement means that at the first sign of printer trouble, many of us just dump the thing and buy a new one. But we ve continued this way for years.

Now, though, ink alternatives throw ink-onomics off balance. Major retailers such as Amazon and Wal-Mart sell off-brand inks dirt cheap. Printer makers say this ink can cause printing problems and bring down the quality of printouts, but the price differences are staggering.

A basic Epson model, the Expression XP-420 all-in-one scanner/printer, lists for $100 and sells for as little as $60. A set of standard replacement ink cartridges, however, costs around $40. Epson s XL cartridges give you a little break nearly three times the ink for around $80 a set.

But in a search for XP-420 ink on Amazon, most results are for off-brand competitors selling XL cartridges for a third of Epson s price, and sometimes even less.

As a parent who doesn t want to padlock the printer, I turned to off-brand ink. And while I have had one of their cartridges fail, the economics still favors the knockoffs.

Epson s new move is a sly one. Rather than compete on price, the printer maker is dropping the cartridge issue entirely. When you buy an EcoTank printer for instance, the ET-2550, which closely resembles Epson s XP-420 you fill up its four-chambered reservoir with ink from plastic containers included with the printer. There s a satisfying feeling of dumping all of that ink into the tubs. You then let the printer prime itself and your ink worries are over.

Fast forward two very print-productive years. You and your family have churned out more than 35 black-and-white and 60 color pages every week. Finally, you need more ink. Epson will sell you a whole set of replacement canisters for $52. That same amount of Epson ink, in XL cartridges, would cost more than 10 times as much.

The old model is out the window. Epson s not trying to make money on ink this time around, because it s charging you up front for the printer. The ET-2550 costs $400; its big brother, the ET-4550, which has a fax, a sheet feeder and Ethernet, costs $500.

I asked John Lang, president and CEO of Epson America, why his company was the only one that could do this. After all, it seems like an obvious strategy.

The answer, he said, has to do with hardware: Epson s advantage is its permanent mechanical print heads, as opposed to the disposable thermal ones used by its chief competitors. Because Epson s print heads are always connected to the printer, ink can be piped to them from anywhere a cartridge or a tank on the side of the printer. More important, because they re mechanical and not thermal, they can operate for years without requiring replacement and are less likely to clog.

Epson s biggest competitor, Hewlett-Packard, has a different answer to the ink problem: subscriptions. Ranging from $3 to $10 a month, you can get automatic shipments of ink cartridges based on the pages you print. You pay more if you go over your limit, and can roll over ink if you don t use it all. But it favors printers with very predictable use. H-P s ink subscription may make sense for small-business owners, but even then, Epson s alternative is worth calculating out. To me, the thought of an ink subscription is sickening. It s worth paying a lump sum to avoid a continuing relationship with my printer maker.

Testing these printers has been reassuringly anticlimactic. The ET-2550 and ET-4550 all-in-one scanner/printers behaved normally, and the print output looked almost exactly like what came out of the nearest comparative model, Epson s XP-420. There s a slight difference in the ink the XP-420 uses a pigment-based ink, which means it is waterproof when it dries, while most of the EcoTank printers use dye ink, which makes for nice photos, but may run if

wet.

Photographers looking for precision photo printers should shop up Epson s line a bit, to the Artisan or Stylus series. People who just want black-and-white pages should consider a laser printer. EcoTank printers are meant to be all-purpose workhorses.

Epson s ink gambit doesn t make all printer annoyances go away. Paper is the other part of the equation. There are still the occasional sheet-feeding issues, where two pages get pulled in instead of one. Which is to say, it s still a printer. That s why Epson offers a two-year warranty on the hardware: If anything goes wrong during that time, Epson will swap it out for a new one. After that, you re on your own.

That made me a little sad. After all, we live in an age when it s de rigueur to trash our electronics when they conk out. Buying a printer for $400 rather than $100 should mean planning to keep it longer, and maybe just maybe paying to repair it rather than throwing it out. Epson says it has no system for printer repairs in the U.S., but that if people keep their printers longer, perhaps third-party providers will seize the opportunity.

There is another earth-conscious aspect to this: No more plastic cartridges ending up in the landfill. You re supposed to bring your cartridges in when buying new ones, but most of us (myself included) just toss them in the garbage. With 20 times the ink that comes in a set of cartridges, the ET-2550 EcoTank printer automatically saves you from about 80 little pieces of plastic. If Epson starts selling these printers by the millions, the planet may be spared whole mountains of spent ink cartridges.

But for most people, it s more about the checking account. Here s the math: If you play by Epson s rules, a $100 printer using Epson ink could cost you as much as $800 over two years, so the EcoTank model is just half that. But paying full price for ink cartridges is a broken concept. If you only buy off-brand ink for your $100 printer, your total cost, even after two years, is less than $200.

The decision boils down to this: Will you pay less and deal with the annoyance of changing ink cartridges and the potential bootleg ink failures? Or would you pay a few hundred dollars more up front for a printer that eliminates ink hassles entirely? (At least for a while.)

Official Touchscreen Display Joins Raspberry Pi Range

The Raspberry Pi is very low cost, but all you get for your money is the actual bare-bones device itself. You will still need to add an SD card, cables, a USB keyboard and mouse, and a screen before you can use it some of which you will likely already have lying around at home.

There are numerous add-ons available to buy too, including an official case, and today the Raspberry Pi Foundation introduces one more addition to its range a superb (and affordable) 7 inch

touchscreen display.

Priced at $60/£48, the 800 x 480 screen only requires two connections to the Pi power from the GPIO port and a ribbon cable that connects to the DSI port. The Pi sits behind the screen, and it s a really well thought out design.

Drivers, which support 10-finger touch, and an on screen keyboard, will be integrated into Raspbian OS, so just grab the latest version and you re good to go.

The technical specs of the new screen are as follows:

- 7-inch Touchscreen Display.
- Screen Dimensions: 194mm x 110mm x 20mm (including standoffs)
- Viewable screen size: 155mm x 86mm
- Screen Resolution 800 x 480 pixels
- 10 finger capacitive touch.
- Connects to the Raspberry Pi board using a ribbon cable connected to the DSI port.
- Adapter board is used to power the display and convert the parallel signals from the display to the serial (DSI) port on the Raspberry Pi.

The display is compatible with all three of the latest Pi models the Raspberry PI Model A+, Raspberry Pi Model B+, and Raspberry Pi 2 Model B. If you have an older model, you might want to think about upgrading to a new one. It won t break the bank after all.

Office 2016 for Windows Launches on September 22

iOS isn t the only operating system getting a big Office update this month. Microsoft will release Office 2016 for Windows on September 22nd, offering a number of small but notable updates to the productivity suite. Some of the highlights include real-time editing by multiple people within the desktop apps, as well as new design themes. There s a dark theme and a colorful theme, which basically just makes the apps look like they already do on basically every other platform, with big blue, green, red, or purple bars streaming across the top of each app to correspond with its icon color.

As Microsoft notes in a blog post, it s also releasing new tools for businesses to manage Office and how it s rolled out. That isn t exactly an exciting Office update, but the implication is that it should be easier for businesses to stay relatively up to date.

Microsoft Pushes Windows 10 Upgrade to PCs Without User Consent

Microsoft today confirmed it has been pre-loading the Windows 10 installation bits onto devices whose owners have not "reserved" a copy or expressed interest in the new OS.

The move has upset some users of Windows 7 and Windows 8.1, who have complained that the unsolicited downloads have caused them to exceed their Internet providers' data caps or seized storage space without their consent.

In a statement, Microsoft acknowledged the practice, which was first reported by The Inquirer on Thursday.

"For those who have chosen to receive automatic updates through Windows Update, we help customers prepare their devices for Windows 10 by downloading the files necessary for future installation," a company spokeswoman said in an email. "This results in a better upgrade experience and ensures the customer's device has the latest software. This is an industry practice that reduces time for installation and ensures device readiness."

If Windows 7 or Windows 8.1 device owners have Windows Update set to the default - and Microsoft-recommended - option that lets the operating system download and install security and other bug fixes automatically in the background, Microsoft will push the Windows 10 upgrade files to the drive.

The upgrade, which can range in size from more than 3GB to nearly 6GB, is placed in the hidden "$Windows.~BT" folder, a long-used destination for Windows upgrades. It will sit there, presumably until the user expresses some kind of desire to install Windows 10.

Microsoft has been pre-loading the Windows 10 upgrade on systems since late July, but it was thought that the practice had been limited to PCs whose owners had accepted Microsoft's free offer and "reserved" a copy through an app the Redmond, Wash. company automatically installed this spring and early summer on virtual all consumer PCs running Windows 7 Home and 8.1 Home, and on many machines powered by Windows 7 Professional and Windows 8.1 Pro.

After the Windows 10 upgrade was downloaded to the device, the user was notified through the app that it was ready to install.

This new scheme, however, is vastly different in that the bits are downloaded to the device even though the user has not asked for the upgrade.

Not surprisingly, among the first to notice the I-did-not-ask-for-this upgrade were people who have data caps mandated by their Internet service providers (ISPs), particularly those who relied on a cellular connection to the Internet.

Several commenters in a long thread on Slashdot claimed that they had exceeded their caps because Microsoft downloaded the massive upgrade to their hardware without their approval.

"I had to travel recently, so I took a laptop with [a] clean Windows 8.1 Pro install," wrote one such user, identified only as "X.25" on Slashdot. "At my destination, I purchased a SIM (they only had 1GB data packages) and put it into the 3G/W-Fi router I carry. I powered the laptop, connected to [the] Internet via said router, checked [a] few things, then went away for [a] few

hours. When I got back to [the] apartment, my data package (and Internet connectivity) was killed because [the] Microsoft idiots decided to start downloading Windows 10 even though I have explicitly closed/rejected all the 'offers.'"

Others didn't appreciate the unwelcome guest that dropped into their limited storage space. Anyone with a 128GB SSD (solid-state drive), for example, would be concerned if 5% of their storage capacity was occupied without their okay.

Some also wondered whether Microsoft would take the next logical step by either dunning users with notifications urging them to apply the already-installed upgrade, or make the much more unlikely move of automatically triggering the upgrade.

The former would, frankly, not be that different from what Microsoft has already done with those who accepted the free upgrade and reserved a copy. It's possible that many on the receiving end of such notifications would approve the upgrade, and even appreciate the fact that they did not have to wait for a long download to complete before upgrading. The latter, however, would be unprecedented, and would almost certainly fuel a firestorm of protest.

Microsoft did not immediately reply to follow-up questions about its intentions.

What is also interesting about the upgrade-prep is Microsoft's defense, that it's an "industry practice."

Although that may be true in limited instances - Google's Chrome browser, for example, regularly pre-loads updates, which are then automatically installed the next time the application is launched - as far as Computerworld knows, it's never been done with either an operating system or software that demands installation files of this size. The most common practice for operating systems, by far, is to begin downloading an upgrade only after the user has been notified, and then approved the procedure.

Wes Miller, an analyst with Directions on Microsoft, agreed. "I've seen some tiny apps do it for updates. But not for an OS upgrade," Miller said in an email answer to a question asking whether he recalled any similar examples.

Yet Another Thing Exposed in The Ashley Madison Hack: Ridiculously Bad Passwords

When data from the massive Ashley Madison hack first leaked online, one tiny bright spot was that researchers said the company appeared to use a strong algorithm to encrypt users passwords. But now one group says it already decoded more than 11 million passwords because programming errors in how that encryption was applied left the information less secure than originally thought.

And the passwords unearthed by the decoding hobbyists, known as CynoSure Prime, so far suggest that many who were seeking thrills

on the infidelity-focused site had poor digital hygiene.

The top password uncovered so far: 123456, according to Ars Technica. The other passwords that made the top five aren't much better: 12345, password, DEFAULT, and 123456789.

But those (awful) passwords shouldn't be too surprising: By some surveys, "123456" has been the most popular password uncovered in data breaches during the past two years.

As a quick reminder, using super common passwords makes it much easier for bad guys to just guess their way into your accounts. And it's a bad idea to reuse passwords, too -- otherwise, a malicious hacker might be able to leverage a password uncovered in one breach to break into one of your other personal accounts.

How To Keep Track of Your Passwords Without Going Insane

In light of recent cyber security breaches, here are the best ways to protect your passwords.

We can probably all agree that the password system, as it stands today, just isn't working. With the constant security breaches in the headlines, we're told regularly to beef up our passwords. But even if we know how to make strong passwords, it's a pain to keep track of them all between every bank account, retailer and app demanding its own unique log-in.

So how can you escape password hell? Or at least snap out of your apathy before a hacker steals your information? We've ranked your options from the most low-maintenance to the most rigorous - for people who want to go the extra mile.

Password managers such as Dashlane - which runs on Mac, Windows iOS and Android - are one way to navigate through password hell.

None of the following suggestions are perfect, by any means - just tips for staying sane in a crazy system. But it turns out that there are some surprisingly easy solutions for this very modern problem. And whatever you do, remember: Anything is safer than using the same password over and over again. Even if it's a really good one.

Easy (aka, lazy) methods

1. Write them down.

Alright. This might sound crazy right off the bat. But one really easy way to keep track of your passwords is to write them down - on paper. Yes, conventional wisdom has said for years that that's a bad idea, and you're in huge trouble if you lose your list. But with so many accounts to juggle nowadays, chances are that you'll be tempted to reuse your passwords if you can't remember all of them. So, writing them down isn't so nutty.

Ideally, you should memorize your most important passwords. But even security expert Bruce Schneier has recommended writing down

passwords and treating that list like you would any other valuable document, which is to say with a high degree of security - no sticky notes on your monitor that say "conglomeratebank.com: jdoe/password123."

As illustrated above, there are definitely bad ways to do this. Getting into an account normally means having to know three things: the location of the account, a username and a password. If you can manage it, don't put all three of these pieces of information in the same place. Similarly, don't do silly things like keeping your bank account password next to a credit or debit card that has your bank's name on it.

What if you want to write everything on a spreadsheet stored on your computer? The same rules and risks apply. And if you want to put that file in the cloud, the stakes are even higher. A cloud spreadsheet is not the place for your most sensitive accounts. If you must do this, confine your cloud spreadsheet to the accounts you would be reasonably okay with getting hacked. And at a minimum, name the file something other than "Passwords."

2. Rely on a major company such as Facebook, Twitter or Google to log-in.

Another easy option is to place your faith in a company like Google, Facebook or Twitter and use their networks to log in to other sites whenever possible. You know those "Log in with Facebook" buttons?

That's what we're talking about here. It won't work for every site, but social network log-in is widespread enough that it could definitely cut down the amount of passwords you have. If you do opt for this method, though, make sure that the password you use for your social network of choice is rock-solid.

3. Reset your password - every time.

And finally, one simple - admittedly inconvenient - method is to go through the "Forgot your password?" spiel each time you log into some sites. That's too much of a pain for sites you use frequently, such as your e-mail or your bank. But it's not a bad fallback strategy for those services you use less often and are most likely to forget anyway - such as the account you made at a retailer's Web site to get free shipping that one time.

Advanced

1. Password managers

There are a number of services that will help you manage your passwords, such as 1Password, LastPass or Dashlane, though you'll have to pay a fee for some features. These services all differ slightly but work on the same basic principle: Each is an online storage locker of your passwords, all hidden behind a single password that only you know (meaning you can't recover your master password from anywhere but your brain). Password managers also offer other perks, such as a place to store secure notes, credit card numbers or information for filling in Web sites. You just have to install the programs into your Web browsers to

record your login information as you surf.

LastPass is free, but costs $12 a year if you want to sync passwords on multiple devices, such as between your phone and computer. It runs on a variety of platforms, including Mac, Windows, iOS, Android and Blackberry. (Courtesy of LastPass)

Password managers are convenient, and will even randomly generate strong passwords, such as "eG7nIs0daud3Taw," for your accounts and then remember those crazy things for you in their vaults. To access your various passwords as you surf, all you have to do is click on a handy button on your browser and choose which account you need to fill in your information.

Each has its strengths and weaknesses. Dashlane is probably the easiest to use and the prettiest to look at. LastPass is compatible with a wide range of devices. And 1Password is comprehensive but expensive.

How much do they cost? 1Password has a one-time $50 cost for Mac or Windows, $18 for iOS and $10 for a full version of the app on Android devices. LastPass and Dashlane are free, but if you want to sync across multiple devices - say your cellphone and your computer - you'll need to upgrade to the premium versions. LastPass costs $12 a year; Dashlane costs $30 a year.

1Password, by AgileBits, has versions for iOS, Android, Mac and Windows.

The two main downsides to password managers are that one, yes, you're still storing everything in one place and depending heavily on that service's security. And second, you're helpless if you don't have access to your locker for some reason - for example, if your employer doesn't let you download software onto your work computer.

2. Isolate your information.

Not that into paying? Another option is to create an e-mail account that's linked to just your most sensitive online accounts - financial accounts, namely - and don't use it for anything else. The fewer ways that criminals can link your various accounts to build a profile of you, the better. Having a separate e-mail account makes it harder for criminals to connect the dots they need to crack security questions, like those that ask for your maiden name or your pets' name. So maybe they won't figure out that the Judy Smith whose banking password they just obtained is the same as the Judy Smith who lists her maiden name and pets' names in her Facebook profile.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for

profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.